(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 May 2004 (06.05.2004)

PCT

(10) International Publication Number
WO 2004/038680 A1

(51) International Patent Classification[7]: G09C 1/00, H04L 9/30, 9/26

(21) International Application Number: PCT/IN2003/000339

(22) International Filing Date: 20 October 2003 (20.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
689/Del/02 26 October 2002 (26.10.2002) IN

(71) Applicant *(for all designated States except US)*: **THE ADDITIONAL DIRECTOR (IPR), DEFENCE RESEARCH & DEVELOPMENT ORGANISATION** [IN/IN]; Ministry of Defence, Government of India, B-341, Sena Bhawan, DHQ PO, New Delhi 110 011, India (IN).

(72) Inventors; and

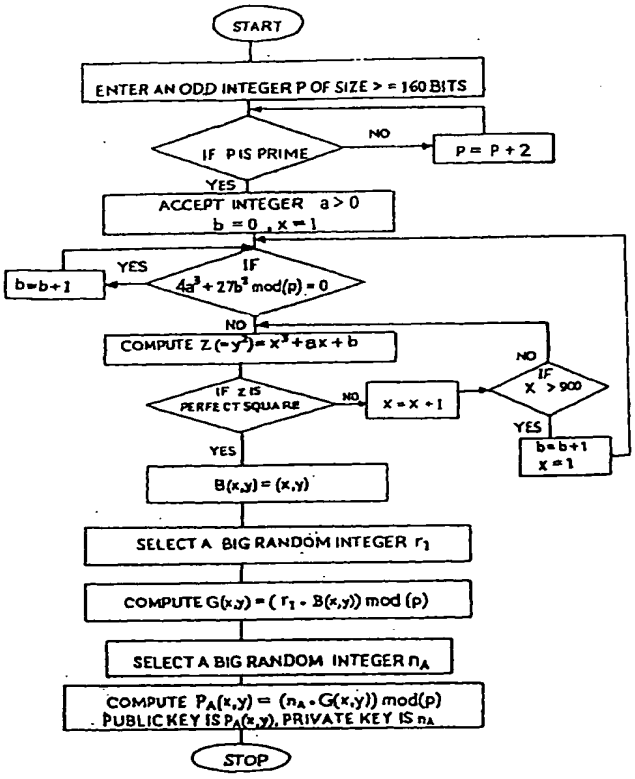
(75) Inventors/Applicants *(for US only)*: **SRUNGARAM, Gopala, Krishna, Murthy** [IN/IN]; Defence Research & Development, Laboratory, Kanchanbagh, Hyderabad 500 058 (IN). **BISWAS, Rathindra, Nath** [IN/IN]; E20/01, Lab Quarters, Kanchanbagh, Hyderabad-500 058 (IN).

(74) Agents: **DAVAR, G., S.** et al.; L.S. Davar & Co., "Monalisa", Flats 1B & 1C, 17 Camac Street, Kolkata 700 017 (IN).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

*[Continued on next page]*

(54) Title: A METHOD OF ELLIPTIC CURVE ENCRYPTION




(57) Abstract: A method of elliptic curve encryption comprising the step of, (a) selecting an elliptic curve $E_p$ (a,b) of the form $y^2=x^3 + ax + b$ mod (p) wherein a and b are non-negative integers less than p satisfying the formula $4a^3 + 27b^2$ mod (p) not equal to 0; (b) generating a large 160 bit random number by a method of concatenation of a number of smaller random numbers; (c) generating a well hidden point G(x,y) on the elliptic curve $E_p$ (a,b) by scalar multiplication of a point B (x,y) on the elliptic curve with a large random integer which further comprises the steps; (i) converting the large random Integer Into a series of powers of $2^{31}$; (ii) converting each coefficient of $2^{31}$ obtained from above step into a binary series; (iii) multiplication of binary series obtained from steps(i) & (ii) above with the point B (x,y) on the elliptic curve ; (d) generating a private key $n_A$(of about>=160 bit length); (e) generating of public key $P_A(x,y)$ given by the formula $P_A(x,y) = (n_A\text{-}G(x,y))$ mod (p); (f) encrypting the input message MSG; (g) decrypting the ciphered text.

WO 2004/038680 A1

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*